***Dr Artur Romaszewski***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*artur.romaszewski@uj.edu.pl*

***Dr hab. med. Wojciech Trąbka***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*wojciech.trabka@uj.edu.pl*

***Mgr Mariusz Kielar***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*mariusz.kielar@uj.edu.pl*

***Mgr Krzysztof Gajda***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*krzysztof.gajda@uj.edu.pl*

# FUNKCJONOWANIE SYSTEMÓW IDENTYFIKACJI I UWIERZYTELNIENIA W POLSKIM SYSTEMIE OPIEKI ZDROWOTNEJ – STAN OBECNY I KIERUNKI ZMIAN

## Wstęp

W chwili obecnej, a więc roku 2017, sytuacja w obszarze ochrony zdrowia, jeżeli chodzi o narzędzia służące do identyfikacji, uwierzytelniania usług w systemach informatycznych i podpisywania elektronicznej dokumentacji medycznej (składania oświadczeń woli) jest nieuregulowana[1]. Generalnie część środowiska świadczącego usługi medyczne wykorzystuje narzędzia dostarczone przez dostawców usług, w tym również dostęp do aplikacji i danych generowanych w trakcie korzystania z systemu w chmurach obliczeniowych. Obecnie nie ma wydawanych przez państwo narzędzi umożliwiających środowisku podmiotów świadczących usługi medyczne i pacjentom identyfikować się w systemie informacji w ochronie zdrowia i potwierdzać zrealizowane tam usługi, identyfikować się w usługach świadczonych w ramach

[1] Za wyjątkiem SIM; Rozporządzenie Ministra Zdrowia z dnia 11 kwietnia 2013 r. w sprawie sposobu identyfikacji usługobiorców, pracowników medycznych i usługodawców oraz sposobu i trybu przekazywania przez usługodawców informacji o pracownikach medycznych udzielających świadczeń opieki zdrowotnej

telemedycyny (telekonsultacji) czy obsługi różnego rodzaju oświadczeń niezbędnych w procesie leczenia takich jak np. składanie świadomej zgody na leczenie czy wskazanie osób uprawnionych do odbioru dokumentacji po śmierci pacjenta. Mimo zalegalizowania telemedycyny w zasadzie nie można uzyskać usługi telekonsultacji z braku możliwości potwierdzenia tożsamości i uprawnień zawodowych osoby zgłaszającej się po wyszukaniu jej w sieci, jako wykonująca zawód medyczny.

Podpisywanie dokumentacji medycznej w postaci elektronicznej odbywa się z poprzez wykorzystanie zakupionych przez podmioty świadczące usługi medyczne, podpisów elektronicznych wydanych w czasie obowiązywania uchylonej w 2016r. ustawy o podpisie elektronicznym tzw. bezpiecznego podpisu (ważnego do końca obowiązywania certyfikatu) lub podpisów elektronicznych uregulowanych, jako usługi zaufania w eIDAS. Nie wykorzystuje się natomiast wymaganych przez eIDAS pieczęci elektronicznych, którymi od roku powinny być opatrywane dokumenty wszystkich podmiotów świadczących usługi zdrowotne (z wyjątkiem indywidualnych działalności osób świadczących usługi medyczne wykorzystujących podpis elektroniczny). Dzieje się tak z dwóch powodów:

- z braku jakiejkolwiek informacji na ten temat ze strony Ministerstwa Zdrowia,
- z braku informacji o możliwość zakupu pieczęci na rynku

Niewątpliwie obecna sytuacja spowodowana jest wielokrotnymi zmianami koncepcji i, co się z tym wiąże, przepisów prawnych, dzięki którym miał funkcjonować system informacji w ochronie zdrowia, którego niezbędnym elementem była prowadzona obowiązkowo we wszystkich podmiotach leczniczych elektroniczna dokumentacja medyczna. Kolejno wycofywano się z planów dowodów ID, następnie z karty specjalisty medycznego, karty specjalisty administracyjnego i elektronicznej karty ubezpieczenia zdrowotnego (KUZ). Karta Specjalisty Medycznego (KSM) to dokument (w postaci karty elektronicznej) umożliwiający identyfikację i uwierzytelnianie pracownika medycznego oraz składanie podpisu elektronicznego pod elektroniczną dokumentacją medyczną, jak również potwierdzający prawo wykonywania zawodu medycznego.

Karta Ubezpieczenia Zdrowotnego miała być samodzielnym dokumentem w postaci karty elektronicznej służącym do weryfikacji statusu ubezpieczeniowego uprawnionego użytkownika karty. Miało to być również narzędzie umożliwiające wyrażanie zgody na udostepnienie elektronicznej dokumentacji medycznej, służące do autoryzacji odbieranych

świadczeń oraz (fakultatywnie) spełniać funkcję nośnika medycznych danych ratunkowych. Obecnie podjęto decyzję o powrocie do koncepcji dowodu osobistego z warstwa elektroniczną oraz o powrocie koncepcji wprowadzenia KSM. Nie przewiduje się wprowadzenia pozostałych rozważanych wcześniej narzędzi. Jednocześnie nowy dowód przejmie niektóre funkcjonalności KUZ i będzie miał zastosowanie w ochronie zdrowia. Implementacja dowodu z warstwą elektroniczną (e-dowodu) była częścią projektu pl.ID, ale nie została ona zrealizowana w uzgodnionym z Komisją Europejską (KE) terminie[2].

Aktualnie powrócono do koncepcji dowodu z warstwą elektroniczną. Nowy elektroniczny dowód osobisty będzie w sposób jednoznaczny i niezaprzeczalny potwierdzał tożsamość osoby, będzie też służył do uwierzytelnienia w e-usługach administracji publicznej oraz do podpisywania dokumentów w cyfrowym świecie. Oprócz tego będzie posiadał aplikację ICAO (dokument podróży z cechą biometryczną „zdjęcie twarzy") i pozwalał potwierdzać obecność w placówkach służby zdrowia. Jednocześnie, z racji ograniczonego zasięgu do jednej grupy zawodowej i chęci szybkiej dystrybucji tych kart, planowana jest do wydania osobna Karta Specjalisty Medycznego (KSM)[3].

Nowy e-dowód zostanie opracowany we współpracy Ministerstwa Cyfryzacji (MC) i Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA), natomiast KSM ma być samodzielnym projektem Ministerstwa Zdrowia (MZ). Będzie on umożliwiał potwierdzenie otrzymania świadczenia opieki zdrowotnej oraz wyrażanie zgody na dostęp do dokumentacji medycznej. Powyższe funkcje były planowane do realizacji na Karcie Ubezpieczenia Zdrowotnego (KUZ). e-Dowód ma przejąć funkcjonalności pierwotnie planowanej Karty Ubezpieczenia Zdrowotnego polegającej na potwierdzeniu wykonania świadczenia opieki zdrowotnej przez pacjenta. Rezultatem takiej konstrukcji ma być wyeliminowanie sytuacji polegających na zgłaszaniu przez świadczeniodawców do zapłaty przez Narodowy Fundusz Zdrowia (NFZ):

[2] Dlatego projekt pl.ID otrzymał status projektu niefunkcjonującego i aby uniknąć konieczności oddania 85% już poniesionych kosztów kwalifikowanych (czyli 148 mln złotych), musi dostarczyć rezultaty – czyli umożliwić rozpoczęcie wydawania e-Dowodów - do końca marca 2019.

[3] Nowa koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną https://mc.gov.pl/aktualnosci/nowa-koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna

- udzielenia świadczeń na rzecz pacjentów, którzy w danym dniu ich nie uzyskali, a w związku z tym nie rejestrowali się u świadczeniodawcy,
- udzielenia fikcyjnych świadczeń tym pacjentom, którzy w danym dniu uzyskali inne, najczęściej „tańsze" świadczenie u danego świadczeniodawcy[4].

Takie prognozowane efekty można będzie jednak uzyskać dopiero po wprowadzeniu obowiązkowego posługiwania się e-dowodem, a więc w obecnie proponowanym wariancie dopiero w 2029 roku. Dlatego MZ i MC pracują nad przygotowaniem alternatywnego rozwiązania na okres przejściowy.

Niezwykle istotne dla systemu opieki zdrowotnej jest proponowana funkcjonalność nowego e-dowodu:

- **Identyfikacja i uwierzytelnienie** obywatela:
  - do systemów informatycznych *on-line* (wymagany będzie PIN), dzięki czemu uzyska się dostęp do wszystkich e-usług administracji publicznej na portalach wykorzystujących węzeł krajowy do identyfikacji elektronicznej (węzeł planowany do wdrożenia w 2017 roku)
  - bezpośrednio do systemu informatycznego administracji publicznej i komercyjnej poprzez interfejs z oprogramowaniem odpowiadającym za komunikację z e-dowodem (o ile dany system zostanie do tego przygotowany; zadanie w gestii opiekunów systemów);
- **Elektroniczne podpisanie dokumentu** przez obywatela w procesach *on-line* z administracją publiczną i służbą zdrowia (podpis serwerowy; wymagany będzie PIN do wcześniejszego uwierzytelnienia przed podpisem);
- **Potwierdzenie obecności obywatela** w procesach z administracją publiczną, służbą zdrowia i innych (bez PIN); właściwie jest to potwierdzenie uczestniczenia e-dowodu w transakcji elektronicznej; możliwe zastosowanie to: uzyskanie dostępu na bramkach w zakładzie pracy, poświadczanie uzyskania przez pacjenta świadczenia medycznego;
- **Możliwość odczytu danych zawartych warstwie wizualnej z warstwy elektronicznej** – w celu pobrania danych do procesu elektronicznego i w celu

[4] Koncepcja: e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych, Załącznik 1: Opis statusu projektu pl.ID

podwyższenia poziomu bezpieczeństwa dokumentu (praktycznie niemożliwe podrobienie danych w warstwie elektronicznej); dostęp do danych będzie zabezpieczony przed przypadkowym odczytem;

- **Możliwość przechowania dodatkowych danych do odczytu** innych, niż w warstwie wizualnej do indywidualnego wykorzystania przez obywatela (np.– z kim kontaktować się w razie wypadku?);

- **Możliwość zainicjowania kwalifikowanego podpisu serwerowego** od dowolnego dostawcy wybranego przez obywatela (uzależnione od udostępnienia takiej opcji przez poszczególnych dostawców podpisów kwalifikowanych); e-dowód (bez opcji z podpisem kwalifikowanym serwerowym) nie zastępuje podpisu kwalifikowanego i nie pozwala z mocy prawa na składanie oświadczeń woli poza administracją publiczną (chyba, że strony komercyjne i obywatel wyrażą zgodę na takie zastosowanie)

- **Będzie parę możliwości użycia e-dowodu** jak m.in. w placówce opieki zdrowotnej – możliwość potwierdzenia tożsamości na komputerze z wewnętrznym albo zewnętrznym **czytnikiem kart bezstykowych**

To, co bardzo istotne dla ochrony zdrowia, to założenie, że e-dowód umożliwi:

- uwierzytelnienie na poziomie wysokim (ang. *high*) - warstwa elektroniczna będzie zawierać certyfikaty do uwierzytelnienia (wymagający PIN) i do potwierdzenia obecności (nie wymagający PIN). Wydawcą certyfikatów będzie Ministerstwo Spraw Wewnętrznych i Administracji i będą one miały ważność równą ważności dokumentu, tj. 10 lat. Certyfikat ten będzie także honorowany przez Ministerstwo Zdrowia na potrzeby wykorzystania w służbie zdrowia
- możliwość złożenia podpisu elektronicznego zgodnego z rozporządzeniem eIDAS dla zaawansowanego podpisu elektronicznego. Nie zakłada się jednak, aby podpis ten był transgraniczną usługą zaufania – będzie on umocowany prawnie w przepisach krajowych do kontaktu z administracją publiczną. Planowane jest wprowadzenia nowej formy podpisu – podpis potwierdzony środkiem identyfikacji. Dopuszczonym środkiem identyfikacji do potwierdzania tego podpisu będzie Profil Zaufany (PZ) i e-dowód
- środek identyfikacji na poziomie wysokim.

Wiele elektronicznych usług wymaga identyfikacji i uwierzytelnienia użytkownika, jednak nie wszystkie te usługi potrzebują takiego samego poziomu bezpieczeństwa. Inne wymagania odnoszą się do dostępu do wrażliwych danych medycznych, inne do pobierania formularzy urzędowych. W zależności od rodzaju usługi i wymaganego poziomu bezpieczeństwa zastosowane powinny być adekwatne metody i techniki uwierzytelnienia o określonej wiarygodności. W związku z tym dla każdej usługi powinien zostać określony (na podstawie analizy ryzyka) poziom wiarygodności wymagany dla procesu uwierzytelnienia. Poziom wiarygodności określa stopień zaufania dopuszczalny i akceptowalny biorąc pod uwagę straty, jakie mogą być poniesione w przypadku błędnego uwierzytelnienia[5].

W rozporządzeniu eIDAS określone zostały trzy poziomy bezpieczeństwa odnoszące się do środka identyfikacji elektronicznej:

- niski poziom bezpieczeństwa,
- średni poziom bezpieczeństwa,
- wysoki poziom bezpieczeństwa.

Stosowane środki identyfikacji elektronicznej (profil zaufany e-PUAP, nowy e-dowód) powinny być adekwatne do potrzeb i celów bezpieczeństwa usługodawców, którzy na podstawie analizy ryzyka określają wystarczające środki potrzebne do zapewnienia bezpieczeństwa ich usług.

Obecnie oferowany przez administrację publiczną środek identyfikacji elektronicznej Profil Zaufany (PZ, e-GO) jest planowany do notyfikacji na poziomie średnim. Jednakże, oczekuje się, że m.in. do obsługi planowanych świadczeń zdrowotnych należy wprowadzić narzędzia do obsługi podwyższonego poziomu zaufania (czyli wysokiego) – w takim przypadku nie będzie możliwe użycie PZ, ale właśnie e-dowodu.

Przykładem usługi wymagającej tego poziomu może być serwis umożliwiający aptekarzowi wydanie leków lub też zatwierdzenie przez osobę z zarządu przedsiębiorstwa dużego transferu pieniędzy z firmowego konta bankowego. W przypadku uwierzytelnienia

[5] Mielnicki T., Wołowski F., Grajek M., Popis P., Identyfikacja i uwierzytelnienie w usługach elektronicznych. https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf

urządzeń czy systemów (tzw. NPE - *Non Person Entity*) wymagane jest użycie certyfikatów elektronicznych (np. X.509 czy CVC)[6]. Profil Zaufany może być stosowany tylko w usługach cyfrowych i bazuje na autoryzacji hasłami jednorazowymi SMS, natomiast e-Dowód będzie mógł być stosowany zarówno w świecie cyfrowym jak i fizycznym, i bazuje na karcie kryptograficznej i autoryzacji PINem.

Główną trudnością w implementacji podpisu kwalifikowanego na karcie jest konieczność zapewnienia możliwości współpracy z dowolnym podmiotem kwalifikowanym działającym w obrębie wspólnego rynku. Ze względu na wymagania bezpieczeństwa niezbędna jest wstępna weryfikacji uprawnień podmiotu kwalifikowanego do dokonania zapisu na karcie. Innym rozwiązaniem jest pozwolenie na umieszczenie w e-dowodzie podpisu kwalifikowanego tylko wybranemu podmiotowi, co rodzi obawy co do nieuprawnionej pomocy państwa albo naruszenia zasad wolnego rynku.

Rozważano możliwość połączenia dowodu osobistego z Kartą Specjalisty Medycznego. Jednak łączenie funkcjonalności Karty Specjalisty Medycznego z elektronicznym dowodem osobistym prowadzi do istotnej komplikacji całego projektu generując dodatkowe ryzyka dla jego realizacji. Ponadto nie ma obiektywnego uzasadnienia dla włączenia do dowodów funkcjonalności KSM przy pominięciu potrzeb innych grup zawodowych. W przyszłości – po przystosowaniu i integracji rejestrów przechowujących informacje o kwalifikacjach zawodowych - e-dowód będzie mógł być też kluczem do tych rejestrów i uwierzytelniać zwrócenie odpowiednich danych. Jednakże dopóki brak jest zintegrowanych centralnych rejestrów kwalifikacji, nie jest to możliwe[7].

Uznano, że wdrożenie KSM jest niezbędne dla upowszechnienia wymiany elektronicznej dokumentacji medycznej istotnej dla podniesienia efektywności służby zdrowia.

W projektowanych zmianach wskazuje się, że brak KUZ i KSM nie uniemożliwia dalszej realizacji projektu P1. Oba zadania (P1 oraz karty) od początku stanowiły niezależne od siebie przedsięwzięcia, aczkolwiek część funkcji kart pełnić miała rolę wspierającą dla P1 i krytyczną dla popularyzacji i upowszechnienia wybranych funkcjonalności P1. Chodzi przede wszystkim o możliwość składania elektronicznego podpisu pod Elektroniczną Dokumentacją Medyczną

[6] Przykład wskazany dla poziomu LoA 4 z normy ISO 29115 w: Tamże
[7] Koncepcja e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych Załącznik 2 Opis planowanej funkcjonalności i architektury IT oraz otoczenie prawno-organizacyjne

(EDM) przez kadrę medyczną (funkcja na KSM) oraz możliwość wyrażania zgody pacjenta na dostęp do jego EDM (pierwotnie funkcja KUZ, obecnie funkcja e-dowodu). Wdrożenie EDM wymaga bowiem nie tylko wprowadzenia stosownego obowiązku na poziomie przepisów, ale też podjęcie odpowiednich działań w zakresie zapewnienia technicznej gotowości interesariuszy do realizacji ww. obowiązku (informatyzacja placówek zdrowia oraz posiadanie narzędzi do elektronicznego podpisu).

Karta Specjalisty Medycznego jest bardzo potrzebnym narzędziem służącym do upowszechnienia dokumentacji medycznej, w tym do wystawiania elektronicznych zwolnień, recept czy skierowań. Karta Specjalisty Medycznego będzie przede wszystkim służyła pracownikowi medycznemu przede wszystkim do składania elektronicznego podpisu pod dokumentacją medyczną. Wydanie KSM wszystkim lekarzom i lekarzom dentystom, a docelowo również przedstawicielom innych zawodów medycznych, będzie wykorzystywane do identyfikacji i uwierzytelniania posiadacza karty w systemach teleinformatycznych, w tym stanowić będzie elektroniczne prawo wykonywania zawodu; karta będzie pozwalała ponadto w przyszłości na dostęp do medycznych danych ratunkowych pacjenta.

Z technicznego punktu widzenia planuje się, że dokument KSM jako "prawo wykonywania zawodu lekarza" i „prawo wykonywania zawodu lekarza dentysty” (w przyszłości planowane jest poszerzenie o kolejne zawody medyczne) powinien być dostępny w dwóch wersjach graficznych (kolorystycznych) dotyczących wersji: na czas odbywania stażu podyplomowego i wersji na czas nieokreślony (biorąc pod uwagę, że dostęp do warstwy elektronicznej nie będzie w pierwszym okresie powszechnie dostępny) i co do zasady zawierać powinien (do uszczegółowienia/modyfikacji na etapie prac legislacyjnych):

- nazwę dokumentu - prawo wykonywania zawodu lekarza i odpowiednio lekarza dentysty;
- nazwę dokumentu w języku angielskim – *“the right to practice the profession of a physician (of a dentist)’;*
- numer prawa wykonywania zawodu lekarza;
- datę uzyskania prawa wykonywania zawodu lekarza;
- wskazanie organu przyznającego prawo wykonywania zawodu lekarza;
- imię i nazwisko lekarza;
- numer PESEL lub w przypadku braku numeru PESEL numer paszportu lub innego dokumentu tożsamości;

- tytuł zawodowy;
- fotografię lekarza, przedstawiającą go bez nakrycia głowy i okularów z ciemnymi szkłami, z naturalnym wyrazem twarzy;
- podpis lekarza;

KSM w warstwie elektronicznej powinna zawierać:

- kontener[8] na certyfikat kwalifikowalny do podpisywania dokumentacji medycznej; certyfikat ten będzie zawierał w dedykowanym polu lub polach (decyzja na etapie projektu technicznego) w postaci jawnej dodatkowe informacje: numer prawa wykonywania zawodu, tytuł, zawód, specjalizacja (jeżeli dotyczy).
- kontener na certyfikat CV do komunikacji z planowaną w przyszłości Kartą Pacjenta (poza zakresem tego projektu),
- kontener na certyfikat do identyfikacji i uwierzytelnienia NFZ/MZ i w systemach placówek medycznych.

Ostateczny zakres danych zostanie ustalony na etapie projektu technicznego i będzie wynikał z brzmienia właściwych przepisów oraz ewentualnych różnic wynikających ze specyfiki poszczególnych zawodów, dla których będą docelowo wydane KSM. Dodatkowo elementami rozwiązania będą system informatyczny do wydawania KSM (system produkcji i personalizacji kart, portal do obsługi zamówień, moduł wydawania certyfikatów) oraz czytniki kart. Karta będzie posiadała tylko interfejs stykowy.

Wprowadzenie funkcjonalności potwierdzania odbioru świadczenia medycznego i udzielania zgody na dostęp do dokumentacji medycznej do dowodów osobistych z warstwą elektroniczną, a także wydanie KSM, wymagać będzie również zmiany szeregu przepisów obowiązujących w systemie ochrony zdrowia, w tym m.in. ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych i ustaw dotyczących poszczególnych zawodów medycznych.

Wśród nowych rozwiązań, które będą mogły być wykorzystywane przez pacjentów, zastosowanie powinna znaleźć usługa tzw. m-dokumentów. Umożliwi ona na korzystanie z

[8] struktura danych, której zadaniem jest przechowywanie w zorganizowany sposób zbioru danych (obiektów). Kontener zapewnia narzędzia dostępu, w tym dodawanie, usuwanie i wyszukiwanie danej (obiektu) w kontenerze. W zależności od przyjętej organizacji, poszczególne kontenery różnią się wydajnością poszczególnych operacji. https://pl.wikipedia.org/wiki/Kontener_(programowanie)

dokumentów potrzebnych m.in. pacjentom w sytuacjach, kiedy potrzebny jest dokument tożsamości lub zdaniem autorów w możliwie niedalekiej przyszłości dokument potwierdzający określone prawa np. znajdowanie się w rejestrze osób posiadających określone uprawnienia (np. krwiodawcy, kombatanci) za pośrednictwem telefonu komórkowego. Usługa jest alternatywą dla tradycyjnego okazywania dokumentu tożsamości lub innego dokumentu w postaci papierowej/plastikowej (np. dowód osobisty)[9].

Projektowane rozwiązanie nie zastępuje tradycyjnego dowodu osobistego czy innych dokumentów potwierdzających uprawnienia, lecz jedynie wprowadza alternatywną możliwość potwierdzania tożsamości przez obywatela. Tym samym obowiązujące regulacje w tym zakresie zostaną jedynie uzupełnione o alternatywny sposób potwierdzenia tożsamości, tj. z wykorzystaniem nowej e-usługi.

Obywatel, w tym pacjent, będzie mógł skorzystać z e-usługi, o ile wyrazi na to zgodę, a zgoda może być cofnięta przez niego w każdym czasie[10]. To, co podkreślają twórcy koncepcji to fakt, że rozwiązanie to jest nie tylko wygodne, ale również w pełni bezpieczne, bowiem żadne dane osobowe nie będą fizycznie przenoszone na nośnik, jakim jest telefon. Samo urządzenie będzie pełniło wyłącznie rolę terminala dostępowego do danych obywatela. Dostęp ten będzie odbywał się na wyraźne życzenie osoby uprawnionej.

Dane będą w pełni wiarygodne, gdyż zostaną pobrane z uwierzytelnionych baz (Rejestr Dowodów Osobistych i innych). Zapewnią więc możliwość identyfikacji i potwierdzenia w takim samym stopniu, jak dziś jest to możliwe przy użyciu tradycyjnych dokumentów.

Poświadczenie tożsamości bądź uprawnień za pomocą m-dokumentów będzie miało dokładnie tę samą wagę i pozwoli na realizację tych samych usług. Dane zawarte na dokumencie w tradycyjnej są zgromadzone i przechowywane w rejestrze publicznym - w przypadku dowodu osobistego w Rejestrze Dowodów Osobistych (RDO). To, co zostanie wyświetlone na urządzeniu podmiotu publicznego będzie niejako cyfrowym odzwierciedleniem np. dowodu osobistego i ma być „zaciągane" z RDO. Należy podkreślić, że dane prezentowane w nowej e-usłudze nie będą przechowywane ani na urządzeniu obywatela, ani na urządzeniu funkcjonariusza czy urzędnika[11].

[9] W brzmieniu nowego art. 16c w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne
[10] Uzasadnienie: https://legislacja.rcl.gov.pl/docs//2/12294950/12413452/12413453/dokument280559.pdf
[11] Informacje o przyczynach i potrzebie wprowadzenia rozwiązań planowanych w projekcie, https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/prace-legislacyjne-rm-i/prace-legislacyjne-rady/wykaz-prac-legislacyjny/rejestr4819738125,dok.html?czas=1487930400

W związku z tym, że pojawiają się narzędzia do identyfikacji, dostawcy potrzebują unikatowej identyfikacji elektronicznej w ramach swoich systemów celem zapewnienia użytkownikom możliwości bezpiecznego korzystania ze świadczonych przez siebie usług[12].

Systemy informatyczne administracji publicznej, w tym w pewnym zakresie także w ochronie zdrowia, do identyfikacji elektronicznej swoich użytkowników wykorzystują:

- mechanizmy zbudowane wewnątrz posiadanych systemów,
- mechanizm profilu zaufanego ePUAP, który - w odniesieniu do usług publicznych - jest aktualnie jedynym powszechnym publicznym środkiem identyfikacji elektronicznej.

W ochronie zdrowia niezwykle istotną sprawą jest przydzielenie odpowiednich uprawnień zarówno przedstawicielom świadczeniodawców, jak i pacjentom, co wiąże się z koniecznością założenia konta w systemie świadczącym określone usługi. W zależności od tego, czego dotyczy usługa *on-line*, identyfikacja elektroniczna zabezpiecza przed jej nieuprawnionym przejęciem lub stworzeniem fałszywej tożsamości i, co za tym idzie, potencjalnego narażenia stron (strony korzystającej z usługi i strony świadczącej usługę) na szkody z tym związane. Z tego powodu, w zależności od zadań wykonywanych w szeroko rozumianym sektorze ochrony zdrowia, stosuje się różne zabezpieczenia właściwe dla świadczonych przez siebie różnych rodzajów usług.

Już obecnie problemem jest istnienie wielu systemów identyfikacji elektronicznej. W związku z tym wydaje się, że normalnym staje się dążenie użytkowników do posługiwania się podobnym lub identycznym zestawem danych identyfikujących w ramach różnych usług. W związku z taką sytuacją podjęto działania, które w rezultacie maja doprowadzić do utworzenia powszechnego systemu identyfikacji elektronicznej i uwierzytelniania, który będzie zarządzany przez odrębny podmiot do tego powołany.

Tworzy się publiczny schemat identyfikacji elektronicznej jako rozwiązanie o charakterze instytucjonalnym, który ma umożliwiać realizację usług publicznych udostępnianych w publicznych systemach teleinformatycznych wymagających uwierzytelnienia. Będzie on obejmował:

- węzeł krajowy oraz

[12] https://legislacja.rcl.gov.pl/projekt/12297458

- przyłączone do niego systemy identyfikacji elektronicznej, w ramach których wydane będą środki identyfikacji elektronicznej (tzw. dostawcy tożsamości) systemy teleinformatyczne, zawierające dane opisujące i identyfikujące osobę, w szczególności rejestry publiczne (tzw. dostawcy atrybutów) oraz systemy teleinformatyczne, w których udostępniane są usługi publiczne (tzw. dostawcy usług). Węzeł krajowy umożliwiać będzie uwierzytelnienie w celu realizacji usługi z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego. Został on przewidziany jako rozwiązanie organizacyjno-techniczne, łączące z jednej strony **platformy,** na których udostępniane są usługi, z drugiej systemy dostarczające **dodatkowe dane identyfikujące osobę**, a z trzeciej - **systemy identyfikacji elektronicznej, w ramach których wydawane będą bezpłatnie środki identyfikacji**[13].

Ważnym obowiązkiem podmiotu odpowiedzialnego za system identyfikacji elektronicznej przyłączony do węzła będzie zapewnienie rozliczalności i niezaprzeczalności działań użytkowników danego środka identyfikacji elektronicznej

Istotnym rozwiązaniem dla ochrony zdrowia jest założenie, że dostawca środka identyfikacji elektronicznej będzie mógł dostarczać możliwie szeroki zakres atrybutów z minimalnego oraz rozszerzonego zestawu danych identyfikujących[14]. W przypadku, gdy dostawca środka identyfikacji elektronicznej nie dysponuje wszystkimi żądanymi atrybutami z rozszerzonego zestawu danych identyfikujących, są one dobierane w procesie identyfikacji elektronicznej od dostawcy atrybutów. Przekazanie dodatkowych atrybutów następuje zawsze za wiedzą i zgodą osoby, której to dotyczy. Zakłada się, że docelowo dostawcy atrybutów będą podłączeni do publicznego schematu identyfikacji elektronicznej za pomocą powstającej Platformy Integracji Usług i Danych[15].

## Piśmiennictwo

[13] Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw – uzasadnienie: https://legislacja.rcl.gov.pl/projekt/12297458
[14] o których mowa w załączniku do Rozporządzenia Wykonawczego Komisji (UE) 2015/1501 dnia 8 września 2015 r. w sprawie ram interoperacyjności.
[15] Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, https://bip.kprm.gov.pl/kpr/form/rejestr14180691990456,dok.html?cza

[1.] https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/prace-legislacyjne-rm-i/prace-legislacyjne-rady/wykaz-prac-legislacyjny/rejestr4819738125,dok.html?czas=1487930400
[2.] https://legislacja.rcl.gov.pl/docs//2/12294950/12413452/12413453/dokument280559.pdf
[3.] https://legislacja.rcl.gov.pl/projekt/12297458
[4.] https://mc.gov.pl/aktualnosci/nowa-koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna
[5.] *Koncepcja e-dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych* Załącznik 2 Opis planowanej funkcjonalności i architektury IT oraz otoczenie prawno-organizacyjne
[6.] *Koncepcja: e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych*, Załącznik 1: Opis statusu projektu pl.ID
[7.] Mielnicki T., Wołowski F., Grajek M., Popis P., *Identyfikacja i uwierzytelnienie w usługach elektronicznych.* https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf
[8.] Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw- uzasadnienie https://legislacja.rcl.gov.pl/projekt/12297458
[9.] Rozporządzenie Ministra Zdrowia z dnia 11 kwietnia 2013 r. w sprawie sposobu identyfikacji usługobiorców, pracowników medycznych i usługodawców oraz sposobu i trybu przekazywania przez usługodawców informacji o pracownikach medycznych udzielających świadczeń opieki zdrowotnej

## *Streszczenie*

W artykule omówione zostały aktualne aspekty dotyczące wykorzystania narzędzi służących do identyfikacji, uwierzytelniania usług w systemach informatycznych i podpisywania elektronicznej dokumentacji medycznej (składania oświadczeń woli) w sektorze opieki zdrowotnej. Wskazano również na nadchodzące kierunki zmian w dotychczasowym modelu zapewniania bezpieczeństwa informacyjnego interesariuszy systemu ochrony zdrowia w Polsce.